



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for IBM Security Access Manager Syslog SmartConnector

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://www.microfocus.com/support-and-services/documentation>

Contents

- Configuration Guide for IBM Security Access Manager Syslog SmartConnector 4
 - Product Overview 4
- Configuration 5
 - Configuring ISAM to Send Audit Events to a Syslog Server 5
 - Prerequisites 5
 - Log Files Containing Special Characters 5
 - Configuration 5
 - Configuring the Syslog SmartConnectors 6
- Installing the SmartConnector 9
 - Preparing to Install the SmartConnector 9
 - Installing and Configuring the SmartConnector 9
- Device Event Mapping to ArcSight Fields13
 - IBM Security Access Manager Audit Mappings to ArcSight ESM Events 14
 - IBM Security Access Manager System Mappings to ArcSight ESM Events 15
- Send Documentation Feedback 16

Configuration Guide for IBM Security Access Manager Syslog SmartConnector

This guide provides information for installing the SmartConnector for IBM Security Access Manager (ISAM) and configuring the device for event collection.

Product Overview

IBM Security Access Manager (ISAM) is a scalable and configurable access management solution which is available as a virtual or hardware appliance. ISAM provides more secure access to web, mobile, and cloud technologies, providing single sign-on across applications and protecting critical assets.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Configuration

This section contains the following topics:

Configuring ISAM to Send Audit Events to a Syslog Server

For complete information about ISAM access auditing and logging, see *IBM Security Access Manager Auditing Topics*, available under [IBM Security Access Manager 9.0 documentation PDFs \(Part 2 of 2\)](#).

Prerequisites

Before configuring ISAM, you might need to complete the following tasks, depending on the nature of your audit configuration.

- Decide on the location of the syslog server if you plan on using a remote machine.
- Make sure that the server certificate was imported into the chosen certificate database if you plan to use a TLS type protocol.
- Make sure that the client certificate to authenticate to the syslog server is trusted by the syslog server. The certificate must be imported into the chosen certificate database.

Log Files Containing Special Characters

Standard XML files should not have special characters. When they do, IBM should escape those characters; otherwise, the connector cannot process those events. For ISAM versions earlier than 9.0.4, these characters are not escaped. This is a bug in ISAM for which IBM has provided a hotfix. Customers using ISAM versions earlier than 9.0.4 should request the hotfix by mentioning APAR IV97992 through their usual IBM support channel.

Configuration

Use the Audit Configuration page of the Security Access Manager user interface to configure auditing.

1. Select **Monitor Analysis and Diagnostics > Logs > Audit Configuration** from the top menu.
2. Select **Enable audit log**.

3. Specify whether the syslog server is on this appliance or on a remote machine. If you select a server other than the local syslog server, provide Host, Port, and Protocol information to identify the server.
4. If you use the default values for tuning, then complete the configuration by clicking **Save**.
5. (Optional) Complete the configuration for Tuning, then click **Save**. For information about tuning, see the *IBM Security Access Manager Auditing Topics* document.

Configuring the Syslog SmartConnectors

Types of ArcSight Syslog SmartConnectors:

- Syslog Daemon
- Syslog Pipe
- Syslog File

Syslog Daemon SmartConnector

The Syslog Deamon SmartConnector is a syslogd-compatible daemon designed to work in operating systems that have no syslog daemon in their default configuration, such as Microsoft Windows. The SmartConnector for Syslog Daemon implements a UDP receiver on port 514 by default, or can be configured on another port to receive syslog events. You can also configure to use the TCP protocol.

To use the SmartConnector for Syslog Daemon, add the following statement in the *rsyslog.conf* file:

```
*.* @@(remote/local-host-IP):514
```

Example: local1.warning @@10.0.0.1:514

- To read all Syslog events, use *.*.
- To filter specific events, replace regex with the specific event name.
- For example: *.* @@(remote/local-host-IP):514 and local1.warning @@10.0.0.1:514.
- To send events over a TCP connection, use @@ and to send events over an UDP connection, use @.

If you are running SmartConnector for Syslog Daemon on the same machine as the server, you must provide the IP address of the local host. If you want to forward events to other machines, you must provide the IP address of the same.

Messages longer than 1024 bytes might be split into multiple messages on syslog daemon. No such restriction exists on syslog file or pipe.

Syslog Pipe and File SmartConnectors

When a syslog daemon is already in place and configured to receive syslog messages, an extra line in the syslog configuration file *rsyslog.conf* can be added to write the events to either a file or a system pipe and the ArcSight SmartConnector can be configured to read the events from it. In this scenario, the ArcSight SmartConnector runs on the same machine as the syslog daemon. The additional configurations for the ArcSight syslog file or syslog pipe SmartConnectors in the system where all Syslog Daemon SmartConnector configurations are done.

The Syslog Pipe SmartConnector is designed to work with an existing syslog daemon. This SmartConnector is especially useful when storage is a factor. In this case, *syslogd* is configured to write to a named pipe, and the Syslog Pipe SmartConnector reads from it to receive events.

The Syslog File SmartConnector is similar to the Pipe SmartConnector. However, this SmartConnector monitors events written to a syslog file such as *messages.log* rather than to a system pipe.

Using the SmartConnector for Syslog Pipe or File

This section provides information to set up your existing syslog infrastructure to send events to the ArcSight Syslog Pipe or File SmartConnector.

The standard UNIX implementation of a syslog daemon reads the configuration parameters from the */etc/rsyslog.conf* file, which contains specific details about which events to write to files, write to pipes, or send to another host.

For Syslog Pipe:

1. Execute the following command to create a pipe:

```
mkfifo /var/tmp/syspipe
```

2. Add one of the following lines depending on your OS to the */etc/rsyslog.conf* file:

```
*.debug /var/tmp/syspipe
```

or

```
*.debug | /var/tmp/syspipe
```

3. Restart the syslog daemon in one of the following methods:

Enter the following commands:

```
/etc/init.d/syslogd stop  
/etc/init.d/syslogd start
```

or

Execute the following command to send a configuration restart signal:

On RedHat Linux:

```
service syslog restart
```

On Solaris:

```
kill -HUP `cat /var/run/syslog.pid`
```

For Syslog File:

1. Create a file or use the default file into which log messages must be written.
2. Modify the /etc/rsyslog.conf file

The syslog daemon is forced to reload the configuration and start writing to the pipe.

3. Restart the syslog daemon in one of the following methods:
 - a. Restart the syslog daemon in one of the following methods:
Enter the following commands:

```
/etc/init.d/syslogd stop  
/etc/init.d/syslogd start
```

or

Execute the following command to send a configuration restart signal:

On RedHat Linux:

```
service syslog restart
```

On Solaris:

```
kill -HUP `cat /var/run/syslog.pid`
```


Installing the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

The syslog SmartConnectors use a sub-connector architecture that lets them receive and process syslog events from multiple devices. There is a unique regular expression that identifies the device. For example, the same SmartConnector can process events from a Cisco Router and a NetScreen Firewall simultaneously. The SmartConnector inspects all incoming messages and automatically detects the type of device that originated the message.

You can install the syslog SmartConnector as a syslog daemon, pipe, or file connector. You can use the Syslog Daemon, Syslog Daemon NG, or Syslog File connector types depending on your requirement. The Syslog File type SmartConnectors also support Syslog Pipe.

Preparing to Install the SmartConnector

Before you install any SmartConnectors, make sure that the OpenText ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, make sure that the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing and Configuring the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.
4. Do one of the following depending on your requirement:

- Select **Syslog Daemon** from the **Type** drop-down:
 - a. Click **Next** and specify the following parameters:

Parameter	Description
Network port	The SmartConnector for Syslog Daemon listens for syslog events from this port.
IP Address	The SmartConnector for Syslog Daemon listens for syslog events only from this IP address, apart from the default (ALL) to bind to all available IP addresses.
Protocol	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
Forwarder	This option applies to Batch Mode only. Specify None , Rename , or Delete as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value None .

- b. Click **Next**.
- Select **Syslog File** from the **Type** drop-down:

a. Click **Next**, and specify the following parameters:

Parameter	Description
Pipe Absolute Path Name	Specify an absolute path to the pipe, or accept the default value: <code>/var/tmp/syspipe</code> .
File Absolute Path Name	<p>Specify the full path name for the file from which this connector will read events. The following are default values:</p> <ul style="list-style-type: none">• Solaris: <code>\var\adm\messages</code>• Linux: <code>\var\log\messages</code> <p>You can use a wildcard pattern in the file name.</p> <p>In the real-time mode, rotation can occur only if the file is over-written or removed from the folder. The real-time processing mode assumes the following external rotation:</p> <ul style="list-style-type: none">• Date format log rotation: The device creates a new log at a specified time in the with the naming convention <code>filename.timestamp.log</code>. The connector detects the new log and terminates the reader thread to the previous log after the processing is complete. The connector then creates a new reader thread to the new <code>filename.timestamp.log</code> and begins processing that file. To enable this log rotation, specify timestamp in <code>yyyy-MM-dd</code> date format. For example, <code>filename.yyyy-MM-dd.log</code>• Index log rotation: The device writes to indexed files in the following format: <code>filename.log.001</code>, <code>filename.log.002</code>, <code>filename.log.003</code>, and so on. At startup, the connector processes the log with highest index. When the device creates a log with a greater index, the connector terminates the reader thread to the previous log after processing completes, creates a thread to the new log, and begins processing that log. To enable this log rotation, use an index format, as shown in the following example: <code>filename '%d,1,99,true'.log</code>; Specifying <code>true</code> indicates that the index can be skipped. For example, if 5 appears before 4, processing proceeds with 5 and will not read 4. Use of <code>true</code> is optional.
Reading Events Real Time or Batch	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
Action Upon Reaching EOF	This option applies to Batch Mode only. Specify None , Rename , or Delete as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value None .
File Extension If Rename Action	This option applies to Batch Mode only. Specify the extension to be added to the file name if the action on reaching the end of file is specified as Rename . The default value is Processed , which adds a <code>.processed</code> extension.

b. Click **Next**.

5. Select a [destination and configure parameters](#).

6. Specify a name for the connector.
7. (Conditional) If you have selected **ArcSight Manager** as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination**, and then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select Do not import the certificate to connector from destination, the connector installation will end.

8. Select whether you want to install the connector as a service or in the standalone mode.
9. Complete the installation.
10. [Run the SmartConnector](#).

For instructions about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. For more information about the ArcSight data fields, see the [ArcSight Console User's Guide](#) .

IBM Security Access Manager Audit 10 Mappings to ArcSight ESM Events

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	high=Failure, low=Success, Pending, Unknown
Destination Host Name	location
Device Custom String 1	extendedDataElements_appliesTo_string_values
Device Custom String 2	extendedDataElements_ruleName_string_values
Device Custom String 3	extendedDataElements_tokenType_string_values
Device Custom String 4	extendedDataElements_issuer_string_values
Device Custom String 5	extendedDataElements_tokenInfo_string_values
Device Custom String 6	sourceComponentId_executionEnvironment
Device Host Name	location
Device Product	'Security Access Manager'
Device Receipt Time	Timestamp
Device Severity	extendedDataElements_outcome_string_children_majorStatus_int_values (0=Success, 1=Failure, 2=Pending, 3=Unknown)
Device Vendor	'IBM'
Event Outcome	extendedDataElements_outcome_string_children_result_string_values
Message	sourceComponentId_component
Name	One of (contextDataElements_name,reporterComponentId_application,"IBM Security Audit Event")
Old File Hash	extendedDataElements_token_string_values
Old File Id	extendedDataElements_actionInfo_noValue_children_actionId_string_values
Request Client Application	sourceComponentId_component
Source User Name	extendedDataElements_userInfoList_noValue_children_appUserName_string_values

IBM Security Access Manager Audit Mappings to ArcSight ESM Events

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	high=Failure, low=Success, Pending, Unknown
Destination Host Name	location
Destination User Name	One of (principal, accessor, accessor_name)
Device Action	outcome (0=Success, 1=Failure, 2=Pending, 3=Unknown)
Device Custom IPv6 Address 2	user_location (Source IPv6 Address)
Device Custom Number 1	resource_access_httpresponse (HTTP Response Code)
Device Custom String 1	principal_auth (Principal Auth)
Device Custom String 2	target_resource (0=AUTHORIZATION, 1=PROCESS, 2=TCB, 3=CREDENTIAL, 5=GENERAL, 6=APPLICATION, 7=AUTHENTICATION) (Resource)
Device Custom String 3	object (Object)
Device Custom String 4	All of (policy_name, policy_type, policy_descr) (Policy Name Type Description)
Device Custom String 5	All of (attribute_name, attribute_type, attribute_source, attribute_value) (Attribute Name Type Source Value)
Device Custom String 6	audit_event (Audit Event)
Device Event Category	component
Device Event Class Id	event_id
Device Host Name	hostname
Device Process Name	originator_blade
Device Product	'Security Access Manager'
Device Receipt Time	date
Device Severity	outcome (0=Success, 1=Failure, 2=Pending, 3=Unknown)
Device Vendor	'IBM'
External Id	action
File Id	session_id
Name	action ((0=Authentication or authorization, 1=Change password, 2=WebSEAL), Management)
Old File Id	outcome_status
Reason	One of (outcome_reason, terminatereason)

ArcSight ESM Field	Device-Specific Field
Request Method	resource_access_httpmethod
Request Url	resource_access_httpurl
Source Address	One of (user_location)
Source Nt Domain	principal_domain

IBM Security Access Manager System Mappings to ArcSight ESM Events

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	high=Error, medium=Warning, low=Informational
Device Custom Number 1	timestamp (Time Stamp)
Device Custom Number 2	eventid (Message Number)
Device Custom String 3	priority (Priority)
Device Custom String 4	eventid (Product Identifiers)
Device Custom String 5	eventid (Component Identifiers)
Device Event Category	name
Device Event Class Id	eventid
Device Host Name	hostname
Device Outbound Interface	interface
Device Product	'Security Access Manager'
Device Receipt Time	date
Device Severity	One of (I=Informational, W=Warning, E=Error)
Device Vendor	'IBM'
File Name	file
Source User Name	user

If the customer used the MySQL JDBC driver 5.1.38 and had issues receiving events, the workaround is to apply the older version of driver 5.0.8, for the connector to start receiving events again.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide for IBM Security Access Manager Syslog SmartConnector (SmartConnectors 8.4.3)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!